Introduction to Discrete Mathematics

Alexander Knop

February 19, 2019

Preface

If you are reading this book, you probably have never studied proofs before. So let me give you some advice: mathematical books are very different from fiction, and even books in other sciences. Quite often you may see that some steps are missing, and some steps are not really explained and just claimed as obvious. The main reason behind this is to make the ideas of the proof more visible and to allow grasping the essence of proofs quickly.

Since the steps are skipped, you cannot just read the book and believe that you studied the topic; the best way to actually study the topic is to try to prove every statement before you read the actual proof in the book. In addition to this, I recommend trying to solve all the exercises in the book (you may find exercises in the middle and at the end of every chapter).

Additionally, many topics in this book have a corresponding five-minute video explaining the material of the chapter, it is useful to watch them before you go into the topic.

Organization

Part 1 covers the basics of mathematics and provide the language we use in the next parts. We start from the explanation of what a mathematical proof is (in Chapter 1). Chapter 2 shows how to prove theorems indirectly using proof by contradiction. Chapter 3 explains the most powerful method in our disposal, proof by induction. Finally, Chapters 4-7 define several important objects such as sets, functions, and relations.

Alexander Knop
San Diego, California, USA

Contents

Part I

Introduction to Mathematical Reasoning

Chapter 1

Proofs

1.1 Direct Proofs

youtu.be/eJD0gGqveIE
What is a Mathematical Proof

We start the discussion of the proofs in mathematics from an example of a proof in “everyday” life. Assume that we know that the following statements are true.

1. If a salmon has fins and scales it is kosher,
2. if a salmon has scales it has fins,
3. any salmon has scales.

Using these facts we may conclude that any salmon is kosher; indeed, any salmon has scales by the third statement, hence, by the second statement any salmon has fins, finally, by the first statement any salmon is kosher since it has fins and scales.

One may notice that this explanation is a sequence of conclusions such that each of them is true because the previous one is true. Mathematical proof is also a sequence of statements such that every statement is true if the previous statement is true. If P and Q are some statements and Q is always true when P is true, then we say that P implies Q. We denote the statement that P implies Q by $P \implies Q$.

In order to define the implication formally let us consider the following table.

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

Let P and Q be some statements. Then this table says that if P and Q are both false, then $P \implies Q$ is true etc.

Exercise 1.1. *Let n be an integer.*

1. *Is it always true that "n^2 is positive" implies "n is not equal to 0"?*
2. *Is it always true that "$n^2 - n - 2$ is equal to 0" implies "n is equal to 2"?*

In the example we gave at the beginning of the section we used some *known* facts. But what does it mean to know something? In math we typically say that we know a statement if we can prove it. But in order to prove this statement we need to know something again, which is a problem! In order to solve it, mathematicians introduced the notion of an *axiom*. An axiom is a statement that is believed to be true and when we prove a statement we prove it under the assumption that these axioms are true[1].

youtu.be/nBjJi6aTk2M
What We Know and How to Find a Proof

For example, we may consider axioms of inequalities for real numbers.

1. Let $a, b \in \mathbb{R}$. Only one of the following is true:
   - $a < b$,
   - $b < a$, or
   - $a = b$.
2. Let $a, b, c \in \mathbb{R}$. Then $a < b$ iff $a + c < b + c$ (iff is an abbreviation for "if and only if").
3. Let $a, b, c \in \mathbb{R}$. Then $a < b$ iff $ac < bc$ provided that $c > 0$ and $a < b$ iff $ac > bc$ if $c < 0$.
4. Let $a, b, c \in \mathbb{R}$. If $a < b$ and $b < c$, then $a < c$.

Let us now try to prove something using these axioms, we prove that if $a > 0$, then $a^2 > 0$. Note that $a > 0$, hence, by the third axiom $a^2 > 0$.

Similarly, we may prove that if $a < 0$, then $a^2 > 0$. And combining these two statements together we may prove that if $a \neq 0$, then $a^2 > 0$.

Such a way of constructing proof is called direct proofs.

Exercise 1.2. *Axiomatic system for a four-point geometry.*
Undefined terms: point, line, is on.
Axioms:

- *For every pair of distinct points x and y, there is a unique line ℓ such that x is on l and y is on l.*
- *Given a line ℓ and a point x that is not on ℓ, there is a unique line m such that x is on m and no point on ℓ is also on m.*

[1]Note that in different parts of math axioms may be different

- *There are exactly four points.*
- *It is impossible for three points to be on the same line.*

Prove that there are at least two distinct lines.

Let n and m be some integers. Using direct proofs we may prove the following two statements.

- if n is even, then nm is also even[2],
- if n is even and m is even, then $n+m$ is also even.

We start from proving the first statement. There is an integer k such that $n = 2k$ since n is even. As a result, $nm = 2(nk)$ so nm is even.

Now we prove the second statement. Since n and m are even there are k and ℓ such that $n = 2k$ and $m = 2\ell$. Hence, $n + m = 2(k + \ell)$ so $n + m$ is even.

1.2 Constructing Proofs Backwards

However, sometimes it is not easy to find the proof. In this case one of the possible methods to deal with this problem is to try to prove starting from the end.

For example, we may consider the statement $(a+b)^2 = a^2+2ba+b^2$. Imagine, for a second, that you have not learned about axioms. In this case you would write something like this:

$$\begin{aligned}(a+b)^2 = (a+b)\cdot(a+b) = &\\ &a(a+b)+b(a+b) = \\ &\qquad a^2+ab+ba+b^2 = a^2+2ba+b^2.\end{aligned}$$

Let us try to prove it completely formally using the following axioms.

1. Let a, b, and c be reals. If $a = b$ and $b = c$, then $a = c$.
2. Let a, b, and c be reals. If $a = b$, then $a + c = b + c$ and $c + a = c + b$.
3. Let a, b, and c be reals. Then $a(b + c) = ab + ac$.
4. Let a and b be reals. Then $ab = ba$.
5. Let a and b be reals. Then $a + b = b + a$.
6. Let a be a real number. Then $a^2 = a \cdot a$ and $a \cdot a = a^2$.
7. Let a be a real number. Then $a + a = 2a$.

[2] A number n is even if there is an integer k such that $n = 2k$.

So the formal proof of the statement $(a+b)^2 = a^2 + 2ab + b^2$ is as follows. First note that $(a+b)^2 = (a+b) \cdot (a+b)$ (by axiom 6), hence, by axiom 1, it is enough to show that $(a+b) \cdot (a+b) = a^2 + 2ab + b^2$. By axiom 3, $(a+b) \cdot (a+b) = (a+b) \cdot a + (a+b) \cdot b$. Axiom 4 implies that $(a+b) \cdot a = a \cdot (a+b)$ and $(a+b) \cdot b = b \cdot (a+b)$ Hence, by axioms 1 and 2 applied twice

$$a \cdot (a+b) + b \cdot (a+b) = (a+b) \cdot a + b \cdot (a+b) = (a+b) \cdot a + (a+b) \cdot b.$$

As a result,

$$(a+b) \cdot (a+b) = (a+b) \cdot a + (a+b) \cdot b = a \cdot (a+b) + b \cdot (a+b) = a \cdot a + a \cdot b + b \cdot a + b \cdot b;$$

so by axiom 1, it is enough to show that $a \cdot a + a \cdot b + b \cdot a + b \cdot b = a^2 + 2ab + b^2$. Additionally, by axiom 6, $a \cdot a = a^2$ and $b \cdot b = b^2$. Hence, by axiom 2, it is enough to show that $a^2 + a \cdot b + b \cdot a + b^2 = a^2 + 2ab + b^2$. By axiom 4, $a \cdot b = b \cdot a$, hence, by axiom 2, $a \cdot b + b \cdot a = b \cdot a + b \cdot a$. Therefore by axiom 7, $a \cdot b + b \cdot a = 2b \cdot a$. Finally, by axiom 2, $a \cdot b + b \cdot a + a^2 + b^2 = 2b \cdot a + a^2 + b^2$ and by axiom 5, $a \cdot b + b \cdot a + a^2 + b^2 = a^2 + a \cdot b + b \cdot a + b^2$ and $2b \cdot a + a^2 + b^2 = a^2 + 2b \cdot a + b^2$. Which finishes the proof by axiom 1.

1.3 Analysis of Simple Algorithms

We can use this knowledge to analyze simple algorithms. For example, let us consider the following algorithm. Let us prove that it is correct i.e. it returns

Algorithm 1 The algorithm that finds the maximum element of a, b, c.

1: **function** MAX(a, b, c)
2:     $r \leftarrow a$
3:     **if** $b > r$ **then**
4:         $r \leftarrow b$
5:     **end if**
6:     **if** $c > r$ **then**
7:         $r \leftarrow c$
8:     **end if**
9:     **return** r
10: **end function**

the maximum of a, b, and c. We need to consider the following cases.

- If the maximum is equal to a. In this case, at line 2, we set $r = a$, at line 3 the inequality $b > r$ is false (since $a = r$ is the maximum) and at line 6 the inequality $c > r$ is also false (since $a = r$ is the maximum). Hence, we do not change the value of r after line 2 and the returned value is a.
- If the maximum is equal to b. We set $r = a$ at line 2. The inequality $b > r$ at line 3 is true (since b is the maximum) and we set r to be equal to b. So at line 6, the inequality $c > r$ is false (since $b = r$ is the maximum). Hence, the returned value is b.

- If the maximum is equal to c. We set $r = a$ at line 2. If the inequality $b > r$ is true at line 3 we set r to be equal to b. So at line 6 the inequality $c > r$ is true (since c is the maximum). Hence, we set r being equal to c and the returned value is c.

1.4 Proofs in Real-life Mathematics

In this chapter we explicitly used axioms to prove statements. However, it leads us to really long and hard to understand proofs (the last example in the previous section is a good example of this phenomenon). Because of this mathematicians tend to skip steps in the proofs when they believe that they are clear. This is the reason why it is arduous to read mathematical texts and it is very different from reading non-mathematical books. A problem that arises because of this tendency is that some mistakes may happen if we skip way too many steps. In the last two centuries there were several attempts to solve this issue, one approach to this we are going to discuss in the second part of this book.

End of The Chapter Exercises

1.3 Using the axioms of inequalities show that if a is a non-zero real number, then $a^2 > 0$.

1.4 Using the axioms of inequalities prove that for all real numbers a, b, and c,

$$bc + ac + ab \leq a^2 + b^2 + c^2.$$

1.5 Prove that for all integers a, b, and c, If a divides b and b divides c, then a divides c. Recall that an integer m divides an integer n if there is an integer k such that $mk = n$.

1.6 Show that square of an even integer is even.

1.7 Prove that 0 divides an integer a iff $a = 0$.

1.8 Using the axioms of inequalities, show that if $a > 0$, b, and c are real numbers, then $b \geq c$ implies that $ab \geq ac$.

1.9 Using the axioms of inequalities, show that if $a, b < 0$ are real numbers, then $a \leq b$ implies that $a^2 \geq b^2$.

Chapter 2

Proofs by Contradiction

2.1 Proving Negative Statements

youtu.be/bWP0VYx75DI
Proofs by Contradiction

The direct method is not very convenient when we need to prove a negation of some statement.

For example, we may try to prove that $78n + 102m = 11$ does not have integer solutions. It is not clear how to prove it directly since we can not consider all possible n and m. Hence, we need another approach. Let us assume that such a solution n, m exists. Note that $78n+102m$ is even, but 11 is odd. In other words, an odd number is equal to an even number, it is impossible. Thus, the assumption was false.

Let us consider a more useful example, let us prove that if p^2 is even, then p is also even (p is an integer). Assume the opposite i.e. that p^2 is even but p is not. Let $p = 2b + 1$[1]. Note that $p^2 = (2b + 1)^2 = 2(2b^2 + 2b) + 1$. Hence, p^2 is odd which contradicts to the assumption that p^2 is even.

Using this idea we may prove much more complicated results e.g. one may show that $\sqrt{2}$ is irrational. For the sake of contradiction, let us assume that it is not true. In other words there are p and q such that $\sqrt{2} = \frac{p}{q}$ and $\frac{p}{q}$ is an irreducible fraction.

Note that $\sqrt{2}q = p$, so $2q^2 = p^2$. Which implies that p is even and 4 devises p^2. Therefore 4 devises $2q^2$ and q is also even. As a result, we get a contradiction with the assumption that $\frac{p}{q}$ is an irreducible fraction.

[1] Note that we use here the statement that an integer n is not even iff it is odd, which, formally speaking, should be proven.

Template for proving a statement by contradiction.

Assume, for the sake of contradiction, that *the statement* is false. Then *present some argument that leads to a contradiction.* Hence, the assumption is false and *the statement* is true.

Exercise 2.1. *Show that* $\sqrt{3}$ *is irrational.*

2.2 Proving Implications by Contradiction

This method works especially well when we need to prove an implication. Since the implication $A \implies B$ is false only when A is true but B is false. Hence, you need to derive a contradiction from the fact that A is true and B is false.

We have already seen such examples in the previous section, we proved that p^2 is even implies p is even for any integer p. Let us consider another example. Let a and b be reals such that $a > b$. We need to show that $(ac < bc) \implies c < 0$. So we may assume that $ac < bc$ but $c \geq 0$. By the multiplicativity of the inequalities we know that if $(a > b)$ and $c > 0$, then $ac > bc$ which contradicts to $ac < bc$.

A special case of such a proof is when we need to prove the implication $A \implies B$, assume that B is false and derive that A is false which contradicts to A (such proofs are called proofs by contraposition); note that the previous proof is a proof of this form.

2.3 Proof of "OR" Statements

Another important case is when we need to prove that at least one of two statements is true. For example, let us prove that $ab = 0$ iff $a = 0$ or $b = 0$. We start from the implication from the right to the left. Since if $a = 0$, then $ab = 0$ and the same is true for $b = 0$ this implication is obvious.

The second part of the proof is the proof by contradiction. Assume $ab = 0$, $a \neq 0$, and $b \neq 0$. Note that $b = \frac{ab}{a} = 0$, hence $b = 0$ which is a contradiction to the assumption.

End of The Chapter Exercises

2.2 Prove that if n^2 is odd, then n is odd.

2.3 In Euclidean (standard) geometry, prove: If two lines share a common perpendicular, then the lines are parallel.

2.4 Let us consider four-lines geometry, it is a theory with undefined terms: point, line, is on, and axioms:

1. there exist exactly four lines,

2. any two distinct lines have exactly one point on both of them, and
3. each point is on exactly two lines.

Show that every line has exactly three points on it.

2.5 Let us consider group theory, it is a theory with undefined terms: group-element and times (if a and b are group elements, we denote a times b by $a \cdot b$), and axioms:

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for every group-elements a, b, and c;
2. there is a unique group-element e such that $e \cdot a = a = a \cdot e$ for every group-element a (we say that such an element is the identity element);
3. for every group-element a there is a group-element b such that $a \cdot b = e$, where e is the identity element;
4. for every group-element a there is a group-element b such that $b \cdot a = e$, where e is the identity element.

Let e be the identity element. Show the following statements

- if $b_0 \cdot a = b_1 \cdot a = e$, then $b_0 = b_1$, for every group-elements a, b_0, and b_1.
- if $a \cdot b_0 = a \cdot b_1 = e$, then $b_0 = b_1$, for every group-elements a, b_0, and b_1.
- if $a \cdot b_0 = b_1 \cdot a = e$, then $b_0 = b_1$, for every group-elements a, b_0, and b_1.

2.6 Let us consider three-points geometry, it is a theory with undefined terms: point, line, is on, and axioms:

1. There exist exactly three points.
2. Two distinct points are on exactly one line.
3. Not all the three points are collinear i.e. they do not lay on the same line.
4. Two distinct lines are on at least one point i.e. there is at least one point such that it is on both lines.

Show that there are exactly three lines.

2.7 Show that there are irrational numbers a and b such that a^b is rational.

2.8 Show that there does not exist the largest integer.

Chapter 3

Proofs by Induction

3.1 Simple Induction

youtu.be/jOnZTWGpX_I
The Induction Principle

Let us consider a simple problem: what is bigger 2^n or n? In this chapter, we are going to study the simplest way to prove that $2^n > n$ for all positive integers n. First, let us check that it is true for small integers n.

n	1	2	3	4	5	6	7	8
2^n	2	4	8	16	32	64	128	256

We may also note that 2^n is growing faster than n, so we expect that if $2^n > n$ for small integers n, then it is true for all positive integers n.

In order to prove this statement formally, we use the following principle.

Principle 3.1 (The Induction Principle)**.** *Let $P(n)$ be some statement about a positive integer n. Hence, $P(n)$ is true for every positive integer n iff*

base case: $P(1)$ *is true and*

induction step: $P(k) \implies P(k+1)$ *is true for all positive integers k.*

Let us prove now the statement using this principle. We define $P(n)$ be the statement that "$2^n > n$". $P(1)$ is true since $2^1 > 1$. Let us assume now that $2^n > n$. Note that $2^{n+1} = 2 \cdot 2^n > 2n \geq n+1$. Hence, we proved the induction step.

Exercise 3.1. *Prove that $(1+x)^n \geq 1 + nx$ for all positive integers n and real numbers $x \geq -1$.*

3.2 Changing the Base Case

Let us consider functions n^2 and 2^n.

n	1	2	3	4	5	6	7	8
n^2	1	4	9	16	25	36	49	64
2^n	2	4	8	16	32	64	128	256

Note that 2^n is greater than n^2 starting from 5. But without some trick we can not prove this using induction since for $n = 3$ it is not true!

The trick is to use the statement $P(n)$ stating that $(n+4)^2 < 2^{n+4}$. The base case when $n = 1$ is true. Let us now prove the induction step. Assume that $P(k)$ is true i.e. $(k+4)^2 < 2^{k+4}$. Note that $2(k+4)^2 < 2^{k+1+4}$ but $(k+5)^2 = k^2 + 10k + 25 \leq 2k^2 + 16k + 32 = 2(k+4)^2$. Which implies that $2^{k+1+4} > (k+5)^2$. So $P(k+1)$ is also true.

In order to avoid this strange +4 we may change the base case and use the following argument.

Theorem 3.1. *Let $P(n)$ be some statement about an integer n. Hence, $P(n)$ is true for every integer $n > n_0$ iff*

base case: $P(n_0 + 1)$ *is true and*

induction step: $P(k) \implies P(k+1)$ *is true for all integers $k > n_0$.*

Using this generalized induction principle we may prove that $2^n \geq n^2$ for $n \geq 5$. The base case for $n = 4$ is true. The induction step is also true; indeed let $P(k)$ be true i.e. $(k+4)^2 < 2^{k+4}$. Hence, $2(k+4)^2 < 2^{k+1+4}$ but $(k+5)^2 = k^2 + 10k + 25 \leq 2k^2 + 16k + 32 = 2(k+4)^2$.

Let us now prove the theorem. Note that the proof is based on an idea similar to the trick with +4, we just used.

Proof of Theorem 3.1. $\Rightarrow$ If $P(n)$ is true for any $n > n_0$ it is also true for $n = n_0 + 1$ which implies the base case. Additionally, it true for $n = k+1$ so the induction step is also true.

$\Leftarrow$ In this direction the proof is a bit harder. Let us consider a statement $Q(n)$ saying that $P(n + n_0)$ is true. Note that by the base case for P, $Q(1)$ is true; by the induction step for P we know that $Q(n)$ implies $P(n+1)$. As a result, by the induction principle $Q(n)$ is true for all positive integers n. Which implies that $P(n)$ is true for all integers $n > n_0$.

□

3.3 Inductive Definitions

We may also define objects inductively. Let us consider the sum $1 + 2 + \cdots + n$ a line of dots indicating "and so on" which indicates the definition by induction. In this case, a more precise notation is $\sum_{i=1}^{n} i$.

Definition 3.1. *Let $a(1), \ldots, a(n), \ldots$ be a sequence of integers. Then $\sum_{i=1}^{n} a(i)$ is defined inductively by the following statements:*

- $\sum_{i=1}^{1} a(i) = a(1)$, *and*
- $\sum_{i=1}^{k+1} a(i) = \sum_{i=1}^{k} a(i) + a(k+1)$.

Let us prove that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Note that by definition $\sum_{i=1}^{1} i = 1$ and $\frac{1(1+1)}{2} = 1$; hence, the base case holds. Assume that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Note that $\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1)$ and by the induction hypothesis $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Hence, $\sum_{i=1}^{n+1} i = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}$.

Exercise 3.2. *Prove that $\sum_{i=1}^{n} 2^i = 2^{n+1} - 2$.*

3.4 Analysis of Algorithms with Cycles

Induction is very useful for analysing algorithms using cycles. Let us extend the example we considered in Section 1.3 on page 6.

Let us consider the following algorithm. We prove that it is working correctly.

Algorithm 2 The algorithm that finds the maximum element of $a_1, \ldots, a_n$.

```
function MAX(a_1, ..., a_n)
    r ← a_1
    for i from 2 to n do
        if a_i > r then
            r ← a_i
        end if
    end for
    return r
end function
```

First, we need to define $r_1, \ldots, r_n$ the value of r during the execution of the algorithm. It is easy to see that $r_1 = a_1$ and $r_{i+1} = \begin{cases} r_i & \text{if } r_i > a_{i+1} \\ a_{i+1} & \text{otherwise} \end{cases}$. Secondly, we prove by induction that r_i is the maximum of $a_1, \ldots, a_i$. It is clear that the base case for $i = 1$ is true. Let us prove the induction step from k to $k+1$. By the induction hypothesis, r_k is the maximum of $a_1, \ldots, a_k$. We may consider two following cases.

- If $r_k > a_{k+1}$, then $r_{k+1} = r_k$ is the maximum of $a_1, \ldots, a_{k+1}$ since r_k is the maximum of $a_1, \ldots, a_k$.
- Otherwise, a_{k+1} is greater than or equal to $a_1, \ldots, a_k$, hence, $r_{k+1} = a_{k+1}$.

Exercise 3.3. *Show that line 6 in the following sorting algorithm executes $\frac{n(n+1)}{2}$ times.*

Algorithm 3 The algorithm is selection sort, it sorts $a_1, \dots, a_n$.

```
function SelectionSort(a_1, ..., a_n)
    for i from 1 to n do
        r ← a_i
        ℓ ← i
        for j from i to n do
            if a_j > r then
                r ← a_j
                ℓ ← j
            end if
        end for
        Swap a_i and a_ℓ.
    end for
end function
```

3.5 Strong Induction

Sometimes $P(k)$ is not enough to prove $P(k+1)$ and we need all the statements $P(1), \dots, P(k)$. In this case we may use the following induction principle.

Theorem 3.2 (The Strong Induction Principle)**.** *Let $P(n)$ be some statement about positive integer n. Hence, $P(n)$ is true for every integer $n > n_0$ iff*

base case: $P(n_0 + 1)$ *is true and*

induction step: *If $P(n_0 + 1), \dots, P(n_0 + k)$ are true, then $P(n_0 + k + 1)$ is also true for all positive integers k.*

Before we prove this theorem let us prove some properties of Fibonacci numbers using this theorem. The Fibonacci numbers are defined as follows: $f_0 = 0$, $f_1 = 1$, and $f_k = f_{k-1} + f_{k-2}$ for $k \geq 2$ (note that they are also defined using strong induction since we use not only f_{k-1} to define f_k).

Theorem 3.3 (The Binet formula)**.** *The Fibonacci numbers are given by the following formula*

$$f_n = \frac{\alpha^n - \beta^n}{\sqrt{5}},$$

where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$.

Proof. We use the strong induction principle to prove this statement with $n_0 = -1$. Let us first prove the base case, $\frac{(\alpha^0 - \beta^0)}{\sqrt{5}} = 0 = f_0$. We also need to prove the induction step.

- If $k = 1$, then $\frac{(\alpha^1 - \beta^1)}{\sqrt{5}} = 1 = f_1$.

- Otherwise, by the induction hypothesis, $f_k = \frac{\alpha^k - \beta^k}{\sqrt{5}}$ and $f_{k-1} = \frac{\alpha^{k-1} - \beta^{k-1}}{\sqrt{5}}$. By the definition of the Fibonacci numbers $f_{k+1} = f_k + f_{k-1}$. Hence,

$$f_{k+1} = \frac{\alpha^k - \beta^k}{\sqrt{5}} + \frac{\alpha^{k-1} - \beta^{k-1}}{\sqrt{5}}.$$

  Note that it is enough to show that

$$\frac{\alpha^{k+1} - \beta^{k+1}}{\sqrt{5}} = \frac{\alpha^k - \beta^k}{\sqrt{5}} + \frac{\alpha^{k-1} - \beta^{k-1}}{\sqrt{5}}. \tag{3.1}$$

  Note that it is the same as

$$\frac{\alpha^{k+1} - \alpha^k - \alpha^{k-1}}{\sqrt{5}} = \frac{\beta^{k+1} - \beta^k - \beta^{k-1}}{\sqrt{5}}.$$

  Additionally, note that α and β are roots of the equation $x^2 - x - 1 = 0$. Hence, $\alpha^{k+1} - \alpha^k - \alpha^{k-1} = \alpha^{k-1}(\alpha^2 - \alpha - 1) = 0$ and $\beta^{k+1} - \beta^k - \beta^{k-1} = \beta^{k-1}(\beta^2 - \beta - 1) = 0$. Which implies equality (3.1).

$\square$

Now we are ready to prove the strong induction principle.

Proof of Theorem 3.2. It is easy to see that if $P(n)$ is true for all $n > n_0$, then the base case and the induction steps are true. Let us prove that if the base case and the induction step are true, then $P(n)$ is true for all $n > n_0$.

Let $Q(k)$ be the statement that $P(n_0 + 1)$, ..., $P(n_0 + k)$ are true. Note that $Q(1)$ is true by the base case for P. Additionally, note that if $Q(k)$ is true, then $Q(k+1)$ is also true, by the induction step for P. Hence, by the induction principle, $Q(k)$ is true for all positive integers k. Which implies that $P(n_0 + k)$ is true for all positive integers k. $\square$

3.6 Recursive Definitions

Sometimes you wish to define objects using objects of the same form like in the case of inductive definitions but you do not know how to enumerate them using an integer parameter.

One example of such a situation is the definition of an arithmetic formula.

base case: x_i is an arithmetic formula on the variables $x_1, \ldots, x_n$ for all i; if c is a real number, then c is also an arithmetic formula on the variables $x_1, \ldots, x_n$.

recursion step: If P and Q are arithmetic formulas on the variables $x_1, \ldots, x_n$, then $(P + Q)$ and $P \cdot Q$ are arithmetic formulas on the variables $x_1, \ldots, x_n$.

Note that this definition implicitly states that any other expressions are not arithmetic formulas.

We can define recursively the value of such a formula. Let $v_1, \ldots, v_n$ be some integers.

base cases: $x_i\big|_{x_1=v_1,\ldots,x_n=v_n} = v_i$; in other words, the value of the arithmetic formula x_i is equal to v_1 when $x_1 = v_1, \ldots, x_n = v_n$; if c is a real number, then $c|_{x_1=v_1,\ldots,x_n=v_n} = c$.

recursion steps: If P and Q are arithmetic formulas on the variables $x_1, \ldots, x_n$, then

$$(P+Q)\big|_{x_1=v_1,\ldots,x_n=v_n} = P\big|_{x_1=v_1,\ldots,x_n=v_n} + Q\big|_{x_1=v_1,\ldots,x_n=v_n}$$

and

$$(P\cdot Q)\big|_{x_1=v_1,\ldots,x_n=v_n} = P\big|_{x_1=v_1,\ldots,x_n=v_n} \cdot Q\big|_{x_1=v_1,\ldots,x_n=v_n}.$$

For example, $((x_1+x_2)\cdot x_3)$ is clearly an arithmetic formula on the variables $x_1, \ldots, x_n$. One may expect the value of this formula with $x_1 = 1$, $x_2 = 0$, and $x_3 = -1$ be equal to -1, let us check:

- Note that
$$\begin{aligned} x_1\big|_{x_1=1,x_2=0,x_3=-1} &= 1, \\ x_2\big|_{x_1=1,x_2=0,x_3=-1} &= 0, \text{ and} \\ x_3\big|_{x_1=1,x_2=0,x_3=-1} &= -1. \end{aligned}$$

- Hence,
$$(x_1+x_2)\big|_{x_1=1,x_2=0,x_3=-1} = 1+0 = 1.$$

- Finally,
$$((x_1+x_2)\cdot x_3)\big|_{x_1=1,x_2=0,x_3=-1} = 1\cdot -1 = -1.$$

A special case of induction which called structural induction is the easiest way to prove properties of recursively defined objects. The idea of this is similar to the idea of strong induction:

- first, we prove the statement for the base case,
- after that we prove the induction step, using the assumption that the statement is true for all the substructures (e.g. subformulas in the previous definition).

To illustrate this method, we prove the following theorem.

Theorem 3.4. *For any arithmetic formula A on x, there is a polynomial p such that $p(v) = A\big|_{x=v}$ for any real value v.*

Proof. **base cases:** If $A = x_i$, then consider the polynomial $p(x) = x$; it is easy to see that $A\big|_{x=v} = v = p(v)$. If $A = c$ where c is a real number, then consider the constant polynomial $p(x) = c$; it is easy to note that $A\big|_{x=v} = c = p(v)$.

induction step: We need to consider two cases. Consider the case when $A = B_1 + B_2$. By the induction hypothesis, there are polynomials q_1 and q_2 such that $B_1\big|_{x=v} = q_1(v)$ and $B_2\big|_{x=v} = q_2(v)$ for all real numbers v. We define $p(x) = q_1(x) + q_2(x)$ (it is a polynomial since sum of two polynomials is a polynomial). It is obvious that $A\big|_{x=v} = B_1\big|_{x=v} + B_2\big|_{x=v} = q_1(v) + q_2(v) = p(v)$.

Another case is $A = B_1 \cdot B_2$. Again, by the induction hypothesis, there are polynomials q_1 and q_2 such that $B_1\big|_{x=v} = q_1(v)$ and $B_2\big|_{x=v} = q_2(v)$ for all real numbers v. We define $p(x) = q_1(x) \cdot q_2(x)$ (it is a polynomial since product of two polynomials is a polynomial). It is obvious that $A\big|_{x=v} = B_1\big|_{x=v} \cdot B_2\big|_{x=v} = q_1(v) \cdot q_2(v) = p(v)$.

□

Exercise 3.4.

- *Define arithmetic formulas with division and define their value (make sure that you handled divisions by* 0*).*
- *Show that for any arithmetic formula with division A on x, there are polynomials p and q such that $\frac{p(v)}{q(v)} = A\big|_{x=v}$ or $A\big|_{x=v}$ is not defined for any real value v.*

3.7 Analysis of Recursive Algorithms

To illustrate the power of recursive definitions and strong induction, let us analyze Algorithm 4. We prove that number of comparisons of this algorithm is bounded by $6 + 2\log_2(n)$. First step of the proof is to denote the worst number of comparisons when we run the algorithm on the list of length n by $C(n)$. It is easy to see that $C(n) = n$ for $n \le 5$. Additionally, $C(n) \le 1 + \max(C(\lfloor \frac{n}{2} \rfloor), C(n - \lfloor \frac{n}{2} \rfloor))$ for $n > 5$. As we mentioned we prove that $C(n) \le 6 + 2\log_2(n)$, we prove it by induction. The base case is clear; let us now prove the induction step. By the induction hypothesis,

$$C(\left\lfloor \frac{n}{2} \right\rfloor) \le 6 + 2\log_2(\left\lfloor \frac{n}{2} \right\rfloor)$$

and

$$C(n - \left\lfloor \frac{n}{2} \right\rfloor) \le 6 + 2\log_2(n - \left\lfloor \frac{n}{2} \right\rfloor).$$

Since $\lfloor \frac{n}{2} \rfloor \le \frac{n}{2}$ and $n - \lfloor \frac{n}{2} \rfloor \le \frac{n}{2} + 1$, $C(n) \le 1 + 2\log_2(\frac{n}{2} + 1)$. However,

$$1 + 6 + 2\log_2\left(\frac{n}{2} + 1\right) \le 6 + 2\log_2\left(\frac{n}{\sqrt{2}} + \sqrt{2}\right) \le 6 + 2\log_2(n)$$

for $n \ge 5$. As a result, we proved the induction step.

Algorithm 4 The binary search algorithm that finds an element e in the sorted list $a_1, \ldots, a_n$.

function BINARYSEARCH(e, a_1, $\ldots$, a_n)
    if $n \leq 5$ **then**
        for i from 1 to n **do**
            if $a_i = e$ **then**
                return i
            end if
        end for
    else
        $\ell \leftarrow \left\lfloor \frac{n}{2} \right\rfloor$
        if $a_\ell \leq e$ **then**
            BINARYSEARCH(e, a_1, $\ldots$, a_ℓ)
        else
            BINARYSEARCH(e, $a_{\ell+1}$, $\ldots$, a_n)
        end if
    end if
end function

End of The Chapter Exercises

3.5 Show that there does not exist the largest integer.

3.6 Show that for any positive integer n, $n^2 + n$ is even.

3.7 Show that for any positive integer n, 3 divises $n^3 + 2n$.

3.8 Show that for any integer $n \geq 10$, $n^3 \leq 2^n$.

3.9 Show that for any positive integer n, $\sum_{i=0}^{n} x^i = \frac{1-x^{n+1}}{1-x}$.

3.10 Show that for any matrix $A \in \mathbb{R}^{m \times n}$ $(n > m)$ there is a nonzero vector $x \in \mathbb{R}^n$ such that $Ax = 0$.

3.11 Show that all the elements of $\{0,1\}^n$ (Binary strings) may be ordered such that every successive strings in this order are different only in one character. (For example, for $n = 2$ the order may be 00, 01, 11, 10.)

3.12 Let $a_0 = 2$, $a_1 = 5$, and $a_n = 5a_{n-1} - 6a_{n-2}$ for all integers $n \geq 2$. Show that $a_n = 3^n + 2^n$ for all integers $n \geq 0$.

3.13 Show that $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ for all integers $n \geq 1$.

3.14 Show that $\sum\limits_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$ for all integers $n \geq 1$.

3.15 Show that $\sum\limits_{i=1}^{n} \frac{1}{i^2} \leq 2 - \frac{1}{n}$ for all integers $n \geq 1$.

3.16 Show that $\sum_{i=1}^{n}(2i-1) = n^2$ for any positive integer n.

3.17 Prove that $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$ for any positive integer n.

3.18 Prove that $\sum\limits_{i=2}^{n}(i+1)2^i = n2^{n+1}$ for all integers $n > 2$.

3.19 Let $a_1, \ldots, a_n$ be a sequence of real numbers. We define inductively $\prod_{i=k}^{n} a_i$ as follows:

- $\prod_{i=1}^{1} a_i = a_1$ and
- $\prod_{i=1}^{k+1} a_i = \left(\prod_{i=1}^{k} a_i\right) \cdot a_{k+1}$.

Prove that $\prod_{i=1}^{n-1}\left(1 - \frac{1}{(i+1)^2}\right) = \frac{n+1}{2n}$ for all integers $n > 1$.

3.20 Let $f_0 = 1$, $f_1 = 1$, and $f_{n+2} = f_{n+1} + f_n$ for all $n \in \mathbb{N}$. Show that $f_n \geq \left(\frac{3}{2}\right)^{n-2}$.

3.21 Show that $f_{n+m} = f_{n-1}f_{m-1} + f_n f_m$.

3.22 Show that two arithmetic formulas $(x_1 + x_2) \cdot x_3$ and $x_1 \cdot x_3 + x_2 \cdot x_3$ on the variables x_1, x_2, and x_3 have the same values.

3.23 We say that L is a list of powers of x iff

- either $L = x^k$ for some positive integer k or
- $L = (x^k, L')$ where L' is a list of powers of x and k is a positive integer.

Let L be a list of powers of x. We say that the sum of L with $x = v$ denoted by $\sum L\big|_{x=v}$

- is equal to x^k whether $L = x^k$ and
- is equal to $x^k + \sum L'\big|_{x=v}$ whether $L = (x^k, L')$.

Prove that for any list L of powers of x there is a polynomial such that $\sum L\big|_{x=v} = p(v)$ for all real numbers v.

Chapter 4

Predicates and Connectives

4.1 Propositions and Predicates

youtu.be/0unvlq2OTaE
Connectives and Propositions

In the previous chapters we used the word "statement" without any even relatively formal definition of what it means. In this chapter we are going to give a semi-formal definition and discuss how to create complicated statements from simple statements.

It is difficult to give a formal definition of what a mathematical statement is, hence, we are not going to do it in this book. The goal of this section is to enable the reader to recognize mathematical statements.

A *proposition* or a mathematical statement is a declarative sentence which is either true or false but not both. Consider the following list of sentences.

1. $2 \times 2 = 4$
2. $\pi = 4$
3. n is even
4. 32 is special
5. The square of any odd number is odd.
6. The sum of any even number and one is prime.

Of those, the first two are propositions; note that this says nothing about whether they are true or not. Actually, the first is true and the second is false. However, the third sentence becomes a proposition only when the value of n is fixed. The fourth is not a proposition. Finally, the last two are propositions (the fifth is true and the sixth is false).

The third statement is somewhat special, because there is a simple way to make it a proposition: one just needs to fix the value of the variables. Such sentences are called predicates and the variables that need to be specified are called free variables of these predicates.

Note that the fourth sentence is also interesting, since if we define what it means to be special, the phrase became a proposition. Mathematicians tend to do such things to give mathematical meanings to everyday words.

4.2 Connectives

Mathematicians often need to decide whether a given proposition is true or false. Many statements are complicated and constructed from simpler statements using *logical connectives*. For example we may consider the following statements:

1. $3 > 4$ and $1 < 1$;
2. $1 \times 2 = 5$ or $6 > 1$.

Logical connective "OR". The second statement is an example of usage of this connective. The statement "P or Q" is true if and only if at least one of P and Q is true. We may define the connective using the truth table of it.

P	Q	P or Q
T	T	T
T	F	T
F	T	T
F	F	F

The or connective is also called *disjunction* and the disjunction of P and Q is often dented as $P \vee Q$.

Warning: Note that in everyday speech "or" is often used in the exclusive case, like in the sentence "we need to decide whether it is an insect or a spider". In this case the precise meaning of "or" is made clear by the context. However, mathematical language should be formal, hence, we always use "or" inclusively.

Logical connective "AND". The first statement is an example of this connective. The statement "P and Q" is true if and only if both P and Q are true. We may define the connective using the truth table of it.

P	Q	P and Q
T	T	T
T	F	F
F	T	F
F	F	F

The or connective is also called *conjunction* and the conjunction of P and Q is often dented as $P \wedge Q$.

> **Warning:** Not all the properties of "and" from everyday speach are captured by logical conjunction. For example, "and" sometimes implies order. For example, "They got married and had a child" in common language means that the marriage came before the child. The word "and" can also imply a partition of a thing into parts, as "The American flag is red, white, and blue." Here it is not meant that the flag is at once red, white, and blue, but rather that it has a part of each color.

Logical connective "NOT". The last connective is called *negation* and examples of usage of it are the following:

1. 5 is not greater than 8;
2. Does not exist an integer n such that $n^2 = 2$.

Note that it is not straightforward where to put the negation in these sentences.

The negation of a statement P is denoted as $\neg P$ (sometimes it is also denoted as $\sim P$).

End of The Chapter Exercises

4.1 Construct truth tables for the statements

- not (P and Q);
- (not P) or (not Q);
- P and (not Q);
- (not P) or Q;

4.2 Consider the statement "All gnomes like cookies". Which of the following statements is the negation of the above statement?

- All gnomes hate cookies.
- All gnomes do not like cookies.
- Some gnome do not like cookies.
- Some gnome hate cookies.
- All creatures who like cookies are gnomes.
- All creatures who do not like cookies are not gnomes.

4.3 Using truth tables show that the following statements are equivalent:

- $P \implies Q$,

- $(P \vee Q) \iff Q$ ($A \iff B$ is the same as $(A \implies B) \wedge (B \implies A)$),
- $(P \wedge Q) \iff P$

4.4 Prove that three connectives "or", "and", and "not" can all be written in terms of the single connective "notand" where "P notand Q" is interpreted as "not (P and Q)" (this operation is also known as Sheffer stroke or NAND).

4.5 Show the same statement about the connective "notor" where "P notor Q" is interpreted as "not (P or Q)" (this operation is also known as Peirce's arrow or NOR).

Chapter 5

Sets

5.1 The Intuitive Definition of a Set

youtu.be/bshBV2H4Sqo
Sets

A set is one of the two most important concepts in mathematics. Many mathematical statements involve “an integer n” or “a real number a”. Set theory notation provides a simple way to express that a is a real number. However, this language is much more expressible and it is impossible to imagine modern mathematics without this notation.

As in the previous chapter it is difficult to define a set formally so we give a less formal definition which should be enough to use the notation. A *set* is a well-defined collection of objects. Important examples of sets are:

1. $\mathbb{R}$ a set of reals,
2. $\mathbb{Z}$ the set of integers[1],
3. $\mathbb{N}$ the set of natural numbers[2],
4. $\mathbb{Q}$ a set of rational numbers,
5. $\mathbb{C}$ a set of complex numbers.

Usually, sets are denoted by single letter.

Objects in a set are called *elements* of the set and we denote the statement “x is in the set E” by the formula $x \in E$ and the negation of this statement by

[1]“Z” stands for the German word Zahlen (“numbers”).

[2]Note that in the literature there are two diffirent traditions: in one 0 is a natural number, in another it is not; in this book we are going to assume that 0 is not a natural number.

$x \notin E$. For example, we proved that $\sqrt{2} \notin \mathbb{Q}$[3].

Exercise 5.1. *Which of the following sets are included in which? Recall that a number is prime iff it is an integer greater than* 1 *and divisible only by* 1 *and itself.*

1. *The set of all positive integers less than* 10.
2. *The set of all prime numbers less than* 11.
3. *The set of all odd numbers greater than* 1 *and less than* 6.
4. *The set of all positive integers less than* 10.
5. *The set whose only elements are* 1 *and* 2.
6. *The set whose only element is* 1.
7. *The set of all prime numbers less than* 11.

5.2 Basic Relations Between Sets

Many problems in mathematics are problems of determining whether two description of sets are describing the same set or not. For example, when we learn how to solve quadratic equations of the form $ax^2 + bx + c = 0$ $(a, b, c \in \mathbb{R})$ we learn how to list the elements of the set $\{x \in \mathbb{R} \,:\, ax^2 + bx + c = 0\}$.

We say that two sets A and B are equal if they contain the same elements (we denote it by $A = B$). If all the elements of A belong to B we say that A is a subset of B and denote it by $A \subseteq B$[4].

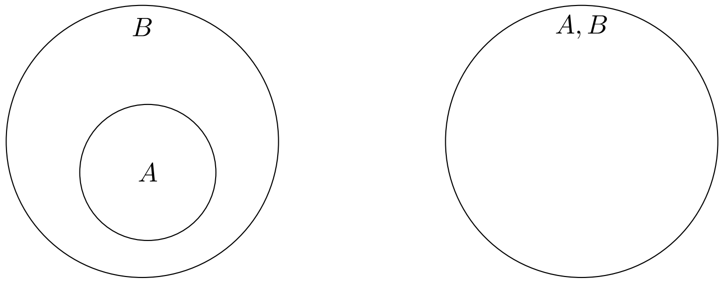
For example, $\mathbb{Q} \subseteq \mathbb{R}$ since any rational number is also a real number. A special set is an empty set i.e. the set that does not have elements, we denote it $\emptyset$.

5.2.1 Diagrams

If we think of a set A as represented by all the points within a circle or any other closed figure, then it is easy to represent the notion of A being a subset of another set B also represented by all the points within a circle. We just put a circle labeled by A inside of the circle labeled by B. We can also diagram an equality by drawing a circle labeled by both A and B. (see fig. 5.1). Such diagrams are called Euler diagrams and it is clear that one may draw Euler diagrams for more than two sets.

[3] The symbol $\in$ was first used by Giuseppe Peano 1889 in his work "Arithmetices principia, nova methodo exposita". Here he wrote on page X: "The symbol $\in$ means is. So $a \in b$ is read as a *is* a b; ..." The symbol itself is a stylized lowercase Greek letter epsilon ("ϵ"), the first letter of the word εστι, which means "is".

[4] In the literature there are three symbols for "subset": $\subseteq$, $\subsetneq$, and $\subseteq$. $A \subseteq B$ means that A is a subset of B and we allow $A = B$ and $A \subsetneq B$ means that A is a subset of B and we forbid $A = B$. However, there is a problem with the third symbol, some people use it as a synonym of $\subseteq$ and some use it as a synonym of $\subsetneq$. Due to this ambiguity we are going to avoid using it in this book.



(a) $A \subseteq B$ (b) $A = B$

Figure 5.1: Euler diagrams

5.2.2 Descriptions of Sets

Listing elements. There are several ways to construct a set, the simplest one is just to list them. For example

1. $\{1, 2, \pi\}$ is the set consisting of three elements 1, 2, and π, and
2. $\{1, 2, 3, \ldots\}$ is the set of all positive integers i.e. it is the set $\mathbb{N}$.

Conditional definitions. We may also describe a set using some constraint e.g we may list all the even numbers using the following formula $\{n \in \mathbb{Z} \;:\; n \text{ is even}\}$ (we read it as "the set of all integers n such that n is even").

Using this we may also define the set of all integers from 1 to m, we denote it $[m]$; i.e. $[m] = \{n \in \mathbb{N} \;:\; 0 < n \leq m\}$.

Constructive definitions. Another way to construct a set of all even numbers is to use the constructive definition of a set: $\{2k \;:\; k \in \mathbb{Z}\}$.

We may also describe a set of rational numbers using this description: $\mathbb{Q} = \{a/b \;:\; a \in \mathbb{Z}, b \in \mathbb{N}\}$ (note that we may also use a mix of a conditional and constructive definitions, $\mathbb{Q} = \{a/b \;:\; a, b \in \mathbb{Z}, b \neq 0\}$).

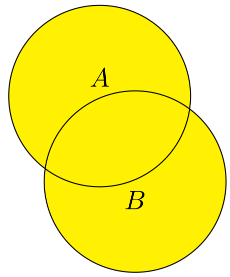
Exercise 5.2. *Describe a set of perfect squares using constructive type of definition.*

5.2.3 Disjoint Sets

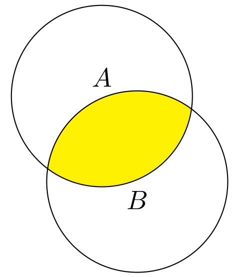
Two sets are *disjoint* iff they do not have common elements. We also say that two sets are *overlapping* iff they are not disjoint i.e. they share an element.

More generally, $A_1, \ldots, A_\ell$ are pairwise disjoint iff A_i is disjoint with A_j for all $i \neq j \in [\ell]$

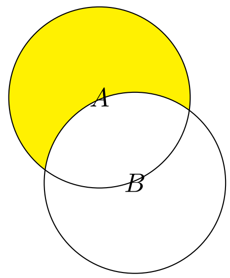
Exercise 5.3. *Of the sets in Exercise 5.1, which are disjoint from which?*



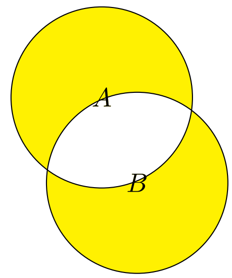
(a) $A \cup B$



(b) $A \cap B$



(c) $A \setminus B$



(d) $A \Delta B$

Figure 5.2: Operations over the sets

5.3 Operations over Sets.

Another way to describe a set is to apply operation to other sets. Let A and B be sets.

The first example of the operations on sets is the *union* operation. The union of A and B is the set containing all the elements of A and all the elements of B i.e. $A \cup B = \{x \ : \ x \in A \text{ or } x \in B\}$[5].

Another example of such an operation is *intersection*. The intersection of A and B is the set of all the elements belonging to both A and B i.e $A \cap B = \{x \ : \ x \in A \text{ and } x \in B\}$[6].

The third operation we are going to discuss this lecture is *set difference*. If A and B are some sets, then $A \setminus B = \{x \ : \ x \in A \text{ and } x \notin B\}$.

The last operation is *symmetric difference*. If A and B are some sets, then $A\Delta B = (A \setminus B) \cup (B \setminus A)$. Note that alternatively $A\Delta B = (A \cup B) \setminus (A \cap B)$

Exercise 5.4. *Describe the set* $\{n \in \mathbb{N} \ : \ n \textit{ is even}\} \cap \{3n \ : \ n \in \mathbb{N}\}$.

[5] Note that this definition is not correct since in the conditional definitions we have to specify the set x belongs to and we cannot do this here.

[6] You may notice that in the definition of the union we use disjunction and in the definition of intersection we use conjunction. Actually this is a the reason the symbol of the conjunction is similar to the symbol of intersection and the symbol of the disjunction is similar to the symbol of union.

Theorem 5.1. *Let A, B, and C be some sets. Then we have the following identities.*

associativity: $A \cup (B \cup C) = (A \cup B) \cup C$ *and* $A \cap (B \cap C) = (A \cap B) \cap C$.

commutativity: $A \cup B = B \cup A$ *and* $A \cap B = B \cap A$.

distributivity: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *and* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof. One may prove these properties using the Euler diagrams. Alternatively they can be proven by definitions. Let us prove only the first part of the distributivity, the rest is Exercise 5.5.

Our proof consists of two parts in the first part we prove that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. Suppose that $x \in A \cup (B \cap C)$. Then $x \in A$ or $x \in (B \cap C)$.

- If $x \in A$, then $x \in (A \cup B)$ and $x \in (A \cup C)$ i.e. $x \in ((A \cup B) \cap (A \cup C))$.
- If $x \in (B \cap C)$, then $x \in B$ and $x \in C$. Which implies that $x \in (A \cup B)$ and $x \in (A \cup C)$. As a result, $x \in ((A \cup B) \cap (A \cup C))$.

□

Exercise 5.5. *Prove the rest of the equalities in Theorem 5.1.*

Probably the most difficult concept connected to sets is the concept of a power set. Let A be some set, then the set of all possible subsets of A is denoted by 2^A (sometimes this set is denoted by $\mathcal{P}(A)$) and called the power set of A. In other words $2^A = \{B \ : \ B \subseteq A\}$.

Warning: Please do not forget about two extremal elements of the power set 2^A: the empty set and A itself.

For example if $A = \{1, 2, 3\}$, then

$$2^A = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

5.4 The Well-ordering Principle

Using the set notation we may finally justify the proof of the statement that $2^n > n$ for all positive integers n from the video about mathematical induction. In order to do this let us first formulate the following theorem.

Theorem 5.2. *Let $A \subseteq \mathbb{Z}$ be a non-empty set. We say that $b \in \mathbb{Z}$ is a lower bound for the set A iff $b \leq a$ for all $a \in A$. Additionally, we say that the set A is bounded if there is a lower bound for A.*

Given this, if A is bounded, then there is a lower bound $a \in A$ for the set A (we say that a is the minimum of the set A).

Note that this theorem also states that any subset of natural numbers have a minimum.

Recall that we wish to prove that $2^n > n$ for all positive n. Assume that it is not true, in this case the set $A = \{n \in \mathbb{N} \ : \ 2^n < n\}$ is non-empty. Denote by n_0 the minimum of the set A, n_0 exists by Theorem 5.2. We may consider the following two cases.

- If $n_0 = 1$, then it leads to a contradiction since $2 = 2^1 > 1$.
- Otherwise, note that $1 \leq n_0 - 1 < n_0$, hence, $2^{n_0-1} > n_0 - 1$. So $2^{n_0} > 2n_0 - 2 \geq n_0$. Which is a contradiction with the definition of n_0.

Finally, we prove Theorem 5.2.

Proof of Theorem 5.2. Let b be a lower bound for the set A. Assume that there is no minimum of the set A. Let $P(n)$ be the statement that $n \notin A$.

First, we are going to prove that $P(n)$ is true for all $n \geq b$. The base case is true since if $b \in A$, then b is the minimum of A which contradicts to the assumption that there is no minimum of A. The induction step is also clear, by the induction hypothesis we know that $P(b)$, $\ldots$, $P(k)$ are true, hence, $(k+1) \in A$ implies that $k+1$ is the minimum of A.

Now we prove that A is empty. Assume the opposite i.e. assume that there is $x \in A$. Note that $x \geq b$ since b is a lower bound of A. However, $P(x)$ is true which implies that $x \notin A$. Therefore the assumption was false and A is empty, but this contradicts to the fact that A is non- empty. $\square$

End of The Chapter Exercises

5.6 Find the power sets of $\emptyset$, $\{1\}$, $\{1,2\}$, $\{1,2,3,4\}$. How many elements in each of this sets?

5.7 Prove that

- $A \subseteq B \iff A \cup B = B$,
- $A \subseteq B \iff A \cap B = A$.

5.8 Let A be a subset of a set U we call this set a universe. We say that the set $\overline{A} = U \setminus A$ is a compliment of A in U. Show the following equalities

- $\overline{\overline{A}} = A$.
- $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
- $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Chapter 6

Functions

youtu.be/VHJeUrCedTU
Functions and Quantifiers

Another important type of objects in mathematics are functions. Function f from a set X to a set Y (we write it as $f : X \to Y$) is a unique assignment of elements of Y to the elements of X. In other words, for each element $x \in X$ there is one assigned element $f(x) \in Y$. We call such an element the *value* of f at x, we also say that $f(x)$ is an *image* of x.

Unfortunately, the definition is not formal. In the rest of the chapter we are going to give a more formal definition.

6.1 Quantifiers.

The first ingredient is called quantifiers. Very often we use phrases like "all the people in the class have smartphones." However, we still do not know how to write it using symbols.

The Universal Quantifier. In order to say "all" or "every" we use the symbol $\forall$: if $P(a)$ is a predicate about $a \in A$, then $\forall a \in A\ P(a)$ is a statement saying that all the elements of A satisfy the predicate P. In other words it is the same as the statement $\{a \in A\ :\ P(a)\} = A$. For example, $\forall x \in \mathbb{R}\ x \cdot 0 = 0$ says that product of every real number and zero is equal to zero.

The Existential Quantifier. The second quantifier means "there is" and denoted by the symbol $\exists$: if $P(a)$ is a predicate about an element of A, then $\exists a \in A\ P(a)$ says that there is an element of A satisfying the predicate P i.e. $\{a \in A\ :\ P(a)\} \neq \emptyset$. For example, $\exists x \in \mathbb{R}\ x^2 - 1 = 0$ states that there is a real solution of the equation $x^2 - 1 = 0$.

Warning: Note that the word "any" sometimes indicates a universal statement and sometimes an existential statement.
Standard meaning of "any" is "ever" like in the statement "$a^2 \geq 0$ for any real number", therefore this statement can be rewritten as $\forall a \in \mathbb{R}\ a^2 \geq 0$. Nonetheless, in the negative and interrogative statements "any" is used to mean "some". For example, "There is not any real number a such that $a^2 < 0$" is asserting that the statement $\exists a \in \mathbb{R}\ a^2 < 0$ is false. And "Is there any real number a such that $a^2 = 1$?" is asking whether the existential statement $\exists a \in \mathbb{R}\ a^2 = 1$ is true.
Real care is required with questions involving "any": "Is there any integer a such that $a \geq 1$?" clearly is asking whether $\exists a \in \mathbb{R}\ a^2 \geq 1$ is true; however, "Is $a \geq 1$ for any integer a" is less clear and might be taken to asking about the same question as the first question, $\exists a \in \mathbb{Z}\ a \geq 1$ (which is true) but might also be taken to be asking about $\forall a \in \mathbb{Z}\ a \geq 1$ (which is false).

6.1.1 Proving Statements Involving Quantifiers

Most of the statements in mathematics involve quantifiers. This is one of the factors distinguishing advanced from elementary mathematics. In this section we give an overview of the main methods of proof. Though the whole book is about proving such results.

Proving statements of the form $\forall a \in A\ P(a)$. Such statements can be rewritten in the form $a \in A \implies P(a)$. For example, we proved earlier that $a^2 \geq 0$ for all real numbers a using this approach.

Proving statements of the form $\exists a \in A\ P(a)$. The easiest way to prove such a statement is by simply exhibiting an element a of A such that $P(a)$ is true. This method is called *proof by example.*

Let us prove the statement $\exists x \in \mathbb{N}\ x^2 = 4$ using this method. Observe that $2 \in N$ and $2^2 = 4$ so $x = 2$ provides an example proving this statement. There are, however, less direct methods such as use of the counting arguments.

Proving statements involving both quantifiers. To illustrate problems of this type let us prove that for any integer n, if n is even, then n^2 is also even.

This statement is a universal statement $\forall n \in \mathbb{Z}$ (n is even $\implies$ n^2 is even). However, the hypothesis that n is even is an existential statement $\exists q \in \mathbb{Z}\ n = 2q$. So we begin the proof as follows:

> Suppose that n is an even integer. Then $n = 2q$ for some integer q.

The conclusion we wish to prove is that n^2 is even, which may be written as $\exists q \in \mathbb{Z}\ n^2 = 2q$. Note that q here is a dummy variable used to express the statement n^2 is a doubled integer. We may replace it by any other letter not already in use, for example $\exists p \in \mathbb{Z}\ n^2 = 2p$. Hence, if we present p such that $n^2 = 2p$ we finish the proof. As a result, we can complete the proof as follows.

Therefore, $n^2 = (2q)^2 = 4q^2$ and so, since $2q^2$ is an integer n^2 is even.

6.1.2 Disproving Statements Involving Quantifiers

Disproving something seems a bit off from the first glance, but to some extent it is the same as proving the negation.

Disproving statements of the form $\forall a \in A\ P(a)$. We may note that the negation of such a statement is the statement $\exists a \in A\ \neg P(a)$. So we can disprove it by giving a single example for which it is false. This is called *Disproof by counterexample* to $P(a)$.

For example, we may disprove the statement $\forall x \in \mathbb{R}\ x^2 > 2$ by giving a counterexample $x = 1$ since $1^2 = 1 < 2$.

Disproving statements of the form $\exists a \in A\ P(a)$. The negation of this statement is the statement $\forall a \in A\ \neg P(a)$. Which gives one way of disproving the statement.

Let us prove that does not exist a real number x such that $x^2 = -1$. We know that, for all $x \in \mathbb{R}$, we have the inequality $x^2 \geq 0$ and so $x^2 \neq -1$. Hence, there does not exist $x \in \mathbb{R}$ such that $x^2 = -1$.

6.2 Cartesian product

Another ingredient is the notion of Cartesian product. If X and Y are two sets, then $X \times Y = \{(x, y)\ :\ x \in X \text{ and } y \in Y\}$. When $X = Y$ we denote $X \times X = X^2$.

Consider the following example. If $X = \{a, b, c\}$ and $Y = \{a, b\}$, then

$$X \times Y = \{(a, a), (a, b), (b, a), (b, b), (c, a), (c, b)\}\,.$$

Additionally, $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is the familiar 2-dimensional Euclidean plane.

Exercise 6.1. *Find the set $\{a, b\} \times \{a, b\} \setminus \{(x, x)\ :\ x \in \{a, b\}\}$*

Theorem 6.1. *For all sets A, B, C, and D the following hold:*

- $A \times (B \cup C) = (A \times B) \cup (A \times C)$*;*
- $A \times (B \cap C) = (A \times B) \cap (A \times C)$*;*
- $(A \times B) \cup (C \times D) \subseteq (A \cup B) \times (C \cup D)$*;*
- $(A \times B) \cap (C \times D) = (A \cap B) \times (C \cap D)$*.*

Proof. It is easy to prove this statement by the definitions. Let us prove only the second equality, the rest is Exercise 6.2.

Note that $(x, y) \in A \times (B \cap C)$ iff $x \in A$ and $y \in (B \cap C)$. Hence, $(x, y) \in A \times (B \cap C)$ iff $x \in A$, $y \in B$, and $y \in C$. Thus $(x, y) \in A \times (B \cap C)$ iff $(x, y) \in (A \times B)$ and $(x, y) \in (A \times C)$. As a result, $(x, y) \in A \times (B \cap C)$ iff $(x, y) \in (A \times B) \cap (A \times C)$ as required. $\square$

Exercise 6.2. *Prove the rest of the equalities in Theorem 6.1.*

6.3 Graphs of Functions

Now we have all the components to define a function. Mathematicians think about the functions in the way we defined them at the beginning of the chapter, however formally in order to define a function $f : X \to Y$ one need to define a set $D \subseteq X \times Y$ (such a set is called the *graph of the function* f) such that

- $\forall x \in X\ \exists y \in Y\ (x, y) \in D$ and
- $\forall x \in X, y_1, y_2 \in Y\ ((x, y_1) \in D \wedge (x, y_2) \implies y_1 = y_2)$.

We say that $y \in Y$ is the value $f(x)$ of the function described by D at $x \in X$ iff $(x, y) \in D$.

The simplest way to think about the functions is in the terms of tables. Let us use this idea to list all the functions $\{a, b, c\}$ to $\{d, e\}$.

x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$	$f_7(x)$	$f_8(x)$
a	d	d	d	d	e	e	e	e
b	d	d	e	e	d	d	e	e
c	d	e	d	e	d	e	d	e

Exercise 6.3. *List all the functions from* $\{a, b\}$ *to* $\{a, b\}$.

However, listing all the values of a function is only possible when the domain of the function is finite. Thus the most common way to describe a function is using a formula which provides a way to find the value of a function. When the function is defined as a formula it is important to be clear which sets are the domain and the codomain of the function.

Let $\mathbb{R}_+ = \{x \in \mathbb{R} : x \geq 0\}$. Consider the following functions.

- $f_1 : \mathbb{R} \to \mathbb{R}$ such that $f_1(x) = x^2$;
- $f_1 : \mathbb{R}_+ \to \mathbb{R}$ such that $f_1(x) = x^2$;
- $f_1 : \mathbb{R} \to \mathbb{R}_+$ such that $f_1(x) = x^2$;
- $f_1 : \mathbb{R}_+ \to \mathbb{R}_+$ such that $f_1(x) = x^2$;

Nonetheless that all these functions are defined using the same formula x^2, we will see in the next chapters that these four functions have different properties.

Exercise 6.4. *Find the graph of the function $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(x) = 3x$.*

Note that when you define the function you need to define it such that the definition makes sense for all the elements of the domain. For example, the formula $g(x) = \frac{x^2-3x+2}{x-1}$ does not define a function from $\mathbb{R}$ to $\mathbb{R}$ since it is not defined for $x = 1$. It is typical to define a function from real numbers to real numbers by a formula and the convention is that the domain is the set of all numbers for which the formula makes sense (unless the domain is specified explicitly). Using this convention the formula g defines a function from $\mathbb{R} \setminus \{1\}$ to $\mathbb{R}$.

If we really need a function from $\mathbb{R}$ there are two possible approaches for extending g.

Rewriting the formula. We can rewrite the formula such that it makes sense for all the real numbers. Note that for all $x \in \mathbb{R} \setminus \{1\}$,

$$\frac{x^2 - 3x + 2}{x - 1} = \frac{(x - 2)(x - 1)}{x - 1} = x - 2.$$

Then $g_1(x) = x - 2$ defines a function on $\mathbb{R}$ extending the function g.

Explicit definition. Alternatively we can explicitly specify the value of g at 1. So

$$g_2(x) = \begin{cases} \frac{x^2-3x+2}{x-1} & \text{if } x \neq 1 \\ -1 & \text{if } x = 1 \end{cases}$$

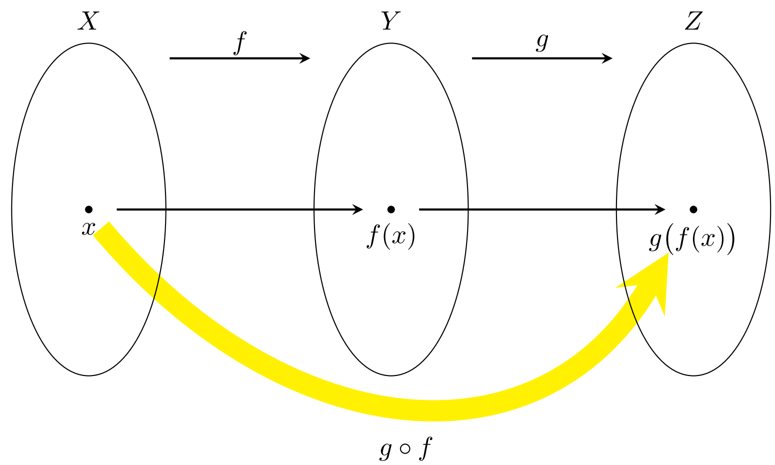
defines a function from $\mathbb{R}$ to $\mathbb{R}$. Note that we can specify the values at individual points any way we want.

Similarly to sets we may define the equality between functions. We say that two functions $f, g : X \to Y$ are equal ($f = g$) iff $f(x) = g(x)$ for all $x \in X$ i.e. their graphs are equal. Note that two functions are equal only if they have the same domains and codomains. For example, g_1 and g_2 we just defined are equal to each other none the less that we defined them in two different ways.

We defined g_1 and g_2 to extend g to a bigger domain, similarly we can make a domain smaller.

Definition 6.1. *Let $f : X \to Y$ and $A \subseteq X$. Then $f|_A : A \to Y$ is a function such that $\forall x \in A$ $f|_A(x) = f(x)$.*

6.4 Composition of Functions



Suppose $f : X\ toY$ and $g : Y \to Z$ be some function. Then, given an element $x \in X$, the function f assigns $y = f(x) \in Y$, and the function g assigns $z = g(y) = g(f(x)) \in Z$. Thus using f and g an element of Z can be assigned to x. This operation defines a function from X to Z and the result of this operation is called the *composition* of f and g.

Definition 6.2. *If $f : X \to Y$ and $g : Y \to Z$, then $h = g \circ f$ is a function from X to Z such that $\forall x \in X\ g(f(x)) = h(x)$.*

.

Let us consider an example. Let $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = x + 1$ and $g : \mathbb{R} \to \mathbb{R}$ such that $g(x) = x^2$. Then $(g \circ f) : \mathbb{R} \to \mathbb{R}$ and $(g \circ f)(x) = (x+1)^2$ for all $x \in \mathbb{R}$. Note that the order of f and g is important since $(f \circ g)(x) = x^2 + 1$. Thus composition is not *commutative*.

There are two special type functions.

- Let $A \subseteq X$, then $i : A \to X$ such that $i(a) = a$ for all $a \in A$ is called the *inclusion* function of A into X. Observe that $(f \circ i) : A \to X$ and $(f \circ i) = f|_A$ for any function $f : X \to Y$.

- Another important function is called the *identity* function. Let X be some set. Then $I_X : X \to X$ is an identity function iff $I_X(x) = x$.

Theorem 6.2. *Let $f : X \to Y$, $g : Y \to Z$, and $h : Z \to W$. Then*

- *$f \circ (g \circ h) = (f \circ g) \circ h$.*

- *$f \circ I_X = f = I_Y \circ f$.*

Proof. These results can be proven simply by evaluating the functions. For example, both functions in the first equality assign $h(g(f(x)))$ for any $x \in X$ and so functions are equal. $\square$

Notice that this theorem states that we may write $f \circ g \circ h$ without ambiguity.

6.5 The Image of a Function

Given a function $f : X \to Y$, it is not necessary that every element of Y is an image of some $x \in X$. For example, the function $\mathbb{R} \to \mathbb{R}$ defined by the formula x^2 does not have -1 as a value.

Thus we may give the following definition.

Definition 6.3. *The image of the function f is defined as follows*

$$Imf = \{y \in Y \ : \ \exists x \in X \ f(x) = y\} = \{f(x) \ : \ x \in X\}$$

(in other words it is the projection of the graph D of f on the second coordinate: $\mathrm{Im} f = \{y \ : \ (x, y) \in D\}$*).*

End of The Chapter Exercises

6.5 Find an image of the function $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(x) = 3x$.

6.6 Determine the following sets:

- $\{m \in \mathbb{N} \ : \ \exists n \in N \ m \leq n\}$;
- $\{m \in \mathbb{N} \ : \ \forall n \in N \ m \leq n\}$;
- $\{n \in \mathbb{N} \ : \ \exists m \in N \ m \leq n\}$;
- $\{n \in \mathbb{N} \ : \ \exists m \in N \ m \leq n\}$.

6.7 Prove or disprove the following statements.

- $\forall m, n \in \mathbb{N} \ m \leq n$.
- $\exists m, n \in \mathbb{N} \ m \leq n$.
- $\exists m \in \mathbb{N} \forall n \in \mathbb{N} \ m \leq n$.
- $\forall m \in \mathbb{N} \exists n \in \mathbb{N} \ m \leq n$.
- $\exists n \in \mathbb{N} \forall m \in \mathbb{N} \ m \leq n$.
- $\forall n \in \mathbb{N} \exists m \in \mathbb{N} \ m \leq n$.

Chapter 7

Relations

Nonetheless that function are used almost everywhere in mathematics, many relations are not functional by their nature. For example, could never define a function $r(a)$ that gives the solution of $x^2 = a$ because there are two solutions for $a > 0$ and there are zero solutions for $a < 0$. A relation is a more general mathematical object.

In order to define a relation we need to relax the definition of the graph of a function (Section 6.3) by allowing more than one "result" and by allowing zero "results". In other words we just say that any set $R \subseteq X_1 \times \cdots \times X_k$ is a k-ary *relation* on $X_1, \ldots, X_k$. We also say that $x_1 \in X_1, \ldots, x_k \in X_k$ are in the relation R iff $(x_1, \ldots, x_k) \in R$. If $k = 2$ such a relation is called a *binary relation* and we write xRy if x and y are in the relation R. If $X_1 = \cdots = X_k = X$, we say that R is a k-ary relation on X.

Note that $=$, $\leq$, $\geq$, $<$, and $>$ define relations on $\mathbb{R}$ (or any subset S of $\mathbb{R}$). For example, if $S = \{0, 1, 2\}$, then $<$ defines the relation $R = \{(0, 1), (0, 2), (1, 2)\}$.

Probably the most popular relation in mathematics is the following relation on $\mathbb{Z}$. Let $a, b \in \mathbb{Z}$. If n divides $a - b$ for some $n \in Z$, we say that "a equivalent to b modulo n" and denote it as $a \equiv b \pmod{n}$. For example, 1 and 4 are equivalent modulo 3 since 3 divides $1 - 4 = -3$.

7.1 Equivalence Relations

The definition of a relation is way to broad. Hence, quite often we consider some types of relation. Probably the most interesting type of the relations is equivalence relations.

Definition 7.1. *Let R be a relation on a set X. We say that R is an equivalence relation if it satisfies the following conditions:*

reflexivity: *xRx for any $x \in X$;*

symmetry: *xRy iff yRx for any $x, y \in X$;*

transitivity: *for any $x, y, z \in X$, if xRy and yRZ, then xRz;*

One may guess that the equivalence relation are mimicking $=$, so it is not a surprise that $=$ is an equivalence relation.

The definition seems quite bizarre, however, all of you are already familiar with an important example: you know that equivalent fractions represent the same number. For example $\frac{2}{4}$ is the same as $\frac{1}{2}$. Let us consider this example more thorough, let S be a set of symbols of the form $\frac{x}{y}$ (note that it is not a set of numbers) where $x, y \in Z$ and $y \neq 0$. We define a binary relation R on S such that $\frac{x}{y}$ and $\frac{z}{w}$ are in the relation R iff $xw = zy$. It is easy to prove that this relation is an equivalence relation.

reflexivity: Let $\frac{a}{b} \in S$. Since $ab = ab$, we have that $\frac{a}{b} R \frac{a}{b}$.

symmetry: Let $\frac{a}{b}, \frac{c}{d} \in S$. Suppose that $\frac{a}{b} R \frac{c}{d}$, by the definition of R, it implies that $ac = db$. As a result, $\frac{c}{d} R \frac{a}{b}$.

transitivity: Let $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in S$ with $\frac{a}{b} R \frac{c}{d}$ and $\frac{c}{d} R \frac{e}{f}$. Then $ad = cb$ and $cf = ed$. The first equality can be rewritten as $c = ad/b$. Hence, $adf/b = ed$ and $af = eb$ since $d \neq 0$. So $\frac{a}{b} R \frac{e}{f}$.

7.1.1 Partitions

Let S be some set. We say that $\{P_1, \ldots, P_k\}$ form a partition of S iff $P_1, \ldots, P_k$ are pairwise disjoint and $P_1 \cup \cdots \cup P_k = S$; in other words, a partition is a way of dividing a set into overlapping pieces.

Exercise 7.1. *Let $\{P_1, \ldots, P_k\}$ be a partition of a set S and R be a binary relation of S such that aRb iff $a, b \in P_i$ for some $i \in [k]$. Show that R is an equivalence relation.*

This exercise shows that one may transform a partition of the set S into an equivalence relation on S. However, it is possible to do the opposite.

Theorem 7.1. *Let R be a binary equivalence relation on a set S. For any element $x \in S$, define $R_x = \{y \in S : xRy\}$ (the set of all the elements of S related to x) we call such a set the equivalence class of x. Then $\{R_x : x \in S\}$ is a partition of S.*

Exercise 7.2. *Prove Theorem 7.1.*

7.1.2 Modular Arithmetic

The relation "$\equiv \pmod{n}$" is actively used in the number theory. One of the important properties of this relation is that it is an equivalence relation.

Theorem 7.2. *The relation $\equiv \pmod{n}$ is an equivalence relation.*

Proof. To prove this statement we need to prove all three properties: reflexivity, symmetry, and transitivity.

reflexivity: Note that for any integer x, $x - x = 0$ is divisible by any integer including n. Hence, $x \equiv x \pmod{n}$.

symmetry: Let us assume that $x \equiv y \pmod{n}$; i.e. $x - y = kn$ for some integer k. Note that $y - x = (-k)n$, so $y \equiv x \pmod{n}$.

transitivity: finally, assume that $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n}$; i.e. $x - y = kn$ and $y - z = \ell n$ for some integers k and ℓ. It is easy to note that $x - z = (x - y) + (y - z) = (k + \ell)n$. As a result, $x \equiv z \pmod{n}$.

Thus, we proved that $\equiv \pmod{n}$ is an equivalence relation. □

Let $x \in \mathbb{Z}$; we denote by $r_{x,n}$ the equivalence class of x with respect to the relation $\equiv \pmod{n}$, we also denote by $\mathbb{Z}/n\mathbb{Z}$ the set of all the equivalence classes with respect to the relation $\equiv \pmod{n}$.

Another important property of these relation is that they behave well with respect to the arithmetic operations.

Theorem 7.3. *Let $x, y \in Z$ and $n \in \mathbb{N}$. Suppose that $a \in r_{x,n}$ and $b \in r_{y,n}$, then $(a + b) \in r_{x+y,n}$ and $ab \in r_{xy,n}$.*

Using this theorem we may define arithmetic operations on the equivalence classes with respect to the relation $\equiv \pmod{n}$. Let $x, y \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then $r_{x,n} + r_{y,n} = \{a + b \ : \ a \in r_{x,n}, b \in r_{y,n}\} = r_{x+y,n}$ and $r_{x,n}r_{y,n} = \{ab \ : \ a \in r_{x,n}, b \in r_{y,n}\} = r_{xy,n}$. Moreover, these operations have plenty of good properties.

Exercise 7.3. *Let $a, b, c \in \mathbb{Z}/n\mathbb{Z}$. Show that the following equalities are true:*

- $a + (b + c) = (a + b) + c$,
- $a + r_{0,n} = a$ *(thus we denote $r_{0,n}$ as 0)*,
- $ar_{1,n} = a$ *(thus we denote $r_{1,n}$ as 1)*,
- *there is a class $d \in \mathbb{Z}/n\mathbb{Z}$ such that $a + d = r_{0,n}$ (thus we denote this d as $-a$)*,
- $a + b = b + a$,
- $ab = ba$,
- $a(b + c) = ab + ac$,

7.2 Partial Orderings

In the previous section we discussed a mathematical way to express the property being similar. In this section we are going to give a way to analyze relation similar to comparisons.

Definition 7.2. *A binary relation R on S is a partial ordering if it satisfies the following constraints.*

reflexivity: *xRx for any $x \in S$;*

antisymmetry: *if xRy and yRx, then $x = y$ for all $x, y \in S$;*

transitivity: *for any $x, y, z \in S$, if xRy and yRZ, then xRz;*

We say that an order R on a set S is total iff for any $x, y \in S$, either xRy or yRx.

Note that if S is a set of numbers, then $\leq$ defines a partial ordering on S; moreover, it defines a total order.

Typically we use symbols similar to $\preceq$ to denote partial orderings and we write $a \prec b$ to express that $a \preceq b$ and $a \neq b$.

Let $\mid$ be the relation on $\mathbb{Z}$ such that $d \mid n$ iff d divides n.

Theorem 7.4. *The relation $\mid$ is a partial ordering of the set $\mathbb{N}$.*

Proof. To prove that this relation is a partial ordering we need to check all three properties.

reflexivity: Note that $x = 1 \cdot x$ for any integer x; hence, $x \mid x$ for any integer x.

antisymmetry: Assume that $x \mid y$ and $y \mid x$. Note that it means that $kx = y$ and $\ell y = x$ for some integers k and ℓ. Hence, $y = (k \cdot \ell)y$ which implies that $k \cdot \ell = 1$ and $k = \ell = 1$. Thus, $x = y$.

transitivity: finally, assume that $x \mid y$ and $y \mid z$; i.e. $kx = y$ and $\ell y = z$. As a result, $(k \cdot \ell)x = z$ and $x \mid z$.

$\square$

Exercise 7.4. *Let S be some set, show that $\subseteq$ defines a partial ordering on the set 2^S.*

7.2.1 Topological Sorting

Partial orderings are very useful for describing complex processes. Suppose that some process consists of several tasks, T denotes the set of these tasks. Some tasks can be done only after some others e.g. when you cooking a salat you need to wash vegetables before you chop them. If $x, y \in T$ be some tasks, $x \preceq y$ if x should be done before y and this is a partial ordering.

In the applications this order is not a total order because some steps do not depend on other steps beeing done first (you can chop tomatos and chop cucumbers in any order). However, if we need to create a schedule in which the tasks should be done, we need to create a total ordering on T. Moreover, this order should be compatible with the partial ordering. In other words, if $x \preceq y$, then $x \preceq_t y$ for all $x, y \in T$, where $\preceq_t$ is the total order. The technique of finding such a total ordering is called *topological sorting*.

Theorem 7.5. *Let S be a finite set and $\preceq$ be a partial order on S. Then there is a total order $\preceq_t$ on S such that if $x \preceq y$, then $x \preceq_t y$ for all $x, y \in S$*

This sorting can be done using the following procedure.

- Initiate the set S beeing equal to T
- Choose the minimal element of the set S with respect to the ordering $\preceq$ (such an element exists since S is a finite set). Add this element to the list, remove it from the set S, and repeate this step if $S \neq \emptyset$.

Let us consider the following example. In the left column we list the classes and in the right column the prerequisite.

Courses	Prerequisite
Math 20A	
Math 20B	Math 20A
Math 20C	Math 20B
Math 18	
Math 109	Math 20C, Math 18
Math 184A	Math 109

We need to find an order to take the courses.

1. We start with
$$S = \{\text{Math 20A}, \text{Math 20B}, \text{Math 20C}, \text{Math 18}, \text{Math 109}, \text{Math 184}\}.$$
There are two minimal elements: Math 20A and Math 18. Let us remove Math 18 from S and add it to the resulting list R.

2. Now we have
$$R = \text{Math 18}$$
and
$$S = \{\text{Math 20A}, \text{Math 20B}, \text{Math 20C}, \text{Math 109}, \text{Math 184}\}.$$
There is only one minimal element Math 20A. We remove it and add it to the list R.

3. On this step
$$R = \text{Math 18}, \text{Math 20A}$$
and
$$S = \{\text{Math 20B}, \text{Math 20C}, \text{Math 109}, \text{Math 184}\}.$$
Again there is only one minimal element: Math 20B.

4.
$$R = \text{Math 18}, \text{Math 20A}, \text{Math 20B}$$
and
$$S = \{\text{Math 20C}, \text{Math 109}, \text{Math 184}\}.$$
There is only one minimal element: Math 20C.

5.
$$R = \text{Math 18}, \text{Math 20A}, \text{Math 20B}, \text{Math 20C}$$
and
$$S = \{\text{Math 109}, \text{Math 184}\}.$$
There is only one minimal element: Math 109.

6. Finally,
$$R = \text{Math 18}, \text{Math 20A}, \text{Math 20B}, \text{Math 20C}, \text{Math 109}$$
and
$$S = \{\text{Math 184}\}.$$
There is only one minimal element: Math 184A.

As a result, the final list is

$$R = \text{Math 18}, \text{Math 20A}, \text{Math 20B}, \text{Math 20C}, \text{Math 109}, \text{Math 184A}.$$

End of The Chapter Exercises

7.5 Show that the relation $|$ does not define a partial ordering on $\mathbb{Z}$.

7.6 Let a relation R be defined on the set of real numbers as follows: xRy iff $2x + y = 3$. Show that it is antisymmetric.

7.7 Are there any minimal elements in $\mathbb{N}$ with respect to $|$? Are there any maximal elements?